ELSEVIER

Journal of Pure and Applied Algebra 139 (1999) 159–182

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Finding the radical of matrix algebras using Fitting decompositions ☆

Gábor Ivanyos

Computer and Automation Institute, Hungarian Academy of Sciences, Lágymányosi u. 11., H-1111 Budapest, Hungary

Received 15 February 1998; received in revised form 1 September 1998

Abstract

We present a new approach to calculating the radical of a matrix algebra, based on the Fitting decomposition with respect to the simultaneous adjoint action of certain commutative subalgebras. This idea results in a reduction to finding the radical of a Lie nilpotent subalgebra or a commutative factor thereof. We also describe a probabilistic version for computing elements which generate the radical as an ideal. © 1999 Elsevier Science B.V. All rights reserved.

MSC: 16N40; 68Q40

1. Introduction

In this paper we address the computational problem of finding the Jacobson radical $Rad(A)$ of a subalgebra A of the full matrix algebra $M_n(K)$ over the field K. In order to simplify discussion, we assume that A contains the identity matrix. We assume that the input is a (small) finite set of matrices which generate A as an algebra and the output is expected to be a set of matrices which generate $Rad(A)$ as an ideal. This task has several applications from modular representation theory of groups to calculation of the structure of Lie algebras. We sketch a deterministic algorithm which works over an arbitrary field with effective arithmetic and reduces the problem of calculating $Rad(A)$ to finding $Rad(B)$ for a commutative algebra B which is a factor of a subalgebra A. The algorithm performs $n^{O(1)}$ operations and is of theoretical interest as the task of

E-mail address: gabor.ivanyos@sztaki.hu (G. Ivanyos)

☆ Research supported by FKFP Grant 0612/1997, OTKA Grants 016503, 022925, NWO-OTKA Grant N26673, and EC Grant ALTEC-KIT.

0022-4049/99/$ – see front matter
PII: S0022-4049(99)00010-9

computing the radical is known to be unsolvable by an algorithm using merely the field operations.

We also present a probabilistic algorithm of Monte Carlo type which works over a sufficiently large perfect ground field where square-free factorization of polynomials can be carried out efficiently. (Examples of such fields are fields of zero characteristic and finite fields.) This appears to be the first attempt to make use of randomization in computing the radical. Provided that the number of generators is small and random elements of A can be generated efficiently the method performs roughly $O(n^4)$ operations in K.

All the known methods for computing the radical are based on solving systems of linear (or semilinear) equations (cf. [5,9,12,18]). The coefficients are the traces (and other invariants in positive characteristic) of the products b_ib_j where $b_1,\dots,b_s$ is a basis of A. Unfortunately it is not known how to determine the coefficients in a way more efficient than computing the diagonal elements of the product b_ib_j for $O(s^2)$ pairs b_i, b_j. Since s can be as large as n^2, the existing algorithms require $\Omega(n^6)$ operations.

The approach of this paper is different. The key idea is very similar to that of [7]: using the Fitting decomposition with respect to the adjoint actions of appropriate subalgebras, we reduce the task to computing the radical of a subalgebra which is nilpotent as a Lie algebra. Factoring by the commutator ideal this leads to a reduction to the commutative case. The probabilistic version is based on the same ideas combined with methods for generating random elements of centralizers of certain subalgebras rather than computing the whole centralizers by solving systems of linear equations.

The paper is structured as follows. In the rest of this section we give a brief description of the computational models we work with and discuss assumptions on random generators for the probabilistic algorithm. Section 2 is devoted to a summary of definitions and known facts from the theory of finite dimensional algebras. The theoretical background of the algorithms is presented in Section 3. The reduction algorithm which works over an arbitrary field can be found in Section 4. Our basic computational tool, an efficient algorithm for generating elements of the centralizer of a single semisimple matrix is presented in Section 5. We conclude with Section 6, where we describe the probabilistic method for finding the radical.

We assume that the field K admits effective procedures for performing the field operations as well as equality tests. The complexity of an algorithm is measured by the number of operations and equality tests required by the algorithm in the worst case. Elementary tasks of linear algebra (matrix multiplication, computing determinants, solving systems of linear equations, etc.) admit efficient solutions in this model, cf. [4]. Let $MM(n) := MM_K(n)$ denote the smallest number of arithmetical operations sufficient to calculate the product of two n by n matrices over K. We assume that $MM(n) \geq n^2$. The standard method shows that $MM(n) = O(n^3)$. Using the asymptotically fastest known (but not very practical) multiplication algorithm we have $MM(n) = O(n^{2.376})$.

It is known [20] that there is no algorithm working in this model which finds the irreducible factors of a polynomial $f(x) \in K[x]$. Even the weaker problem of finding

the square-free part of $f(x)$ (the product of the irreducible factors of $f(x)$) appears to be unsolvable in this model (over a field of positive characteristic). In Section 6 we shall restrict ourselves to fields where this latter task can be effectively solved. For such a field K we denote by $SF_K(n)$ the number of arithmetical operations required to calculate the square-free part of a polynomial of degree n. If K is an arbitrary field of zero characteristic then the square-free part of $f(x)$ is simply $f(x)/gcd(f(x), f'(x))$ and hence $SF_K(n) = n^{1+o(1)}$ (cf. [4]). If K is a finite field then $SF_K(n) = n^{1+o(1)} + O(n \log |K|)$ (cf. [16]).

The probabilistic algorithm of Section 6 assumes the presence of an auxiliary procedure which selects random elements from the algebra A independently. The distribution of the elements is typically concentrated on an appropriate finite subset of A. We do not require uniformity. Instead, we assume randomness in an algebraic sense explained below.

Let U be a finite dimensional vector space over K and let K' be an algebraic closure of K. Let $0 < \delta < 1$ and D be an integer. We say that a probability distribution on U satisfies condition $AlgRand(U, D, \delta)$ if for every nonzero polynomial function $f : K' \otimes_K U \to K'$ of degree at most D the probability of $f(u) = 0$ is at most δ. A possible way to achieve this is the following. Assume that $u_1, \ldots, u_s$ form a K-linear generating system of U. Let Ω be a finite subset of K with $|\Omega| \geq D/\delta$. We take $u = \alpha_1 u_1 + \cdots + \alpha_s u_s$ where the coefficients $\alpha_1, \ldots, \alpha_s$ are drawn uniformly and independently from Ω. Then, by the Schwartz–Zippel lemma [19,22], the probability of $f(u) = 0$ is at most $D/|\Omega| \leq \delta$.

We shall make use of the following lemma. The proof can be carried out in a way analogous to the proof of the Schwartz–Zippel lemma. We leave the details to the reader.

Lemma 1. *Let $0 < \varepsilon < 1$ be a real number. Let $f : U'^k \to K'$ be a nonzero polynomial function of degree at most D. Let $h = \lceil (\log k + \log \frac{1}{\varepsilon})/\log \frac{1}{\delta} \rceil$ and assume that the elements $u_{11}, \ldots, u_{1h}, \ldots, u_{k1}, \ldots, u_{kh} \in U$ are chosen independently according to a probability distribution satisfying $AlgRand(U, D, \delta)$. Then with probability at least $1 - \varepsilon$ there exist indices $j_1, \ldots, j_k \in \{1, \ldots, h\}$ such that $f(u_{1j_1}, \ldots, u_{kj_k}) \neq 0$.*

The probabilistic algorithm of Section 6 requires that the random elements of A are chosen according to a probability distribution satisfying condition $AlgRand(A, n^2, \delta)$ for a constant $0 < \delta < 1$, say $\delta = \frac{1}{2}$. Of course, in this condition it is implicit that the ground field K is sufficiently large (namely $|K| \geq n^2/\delta$). The cost of selecting a single random element is denoted by $R(A)$. For a matrix algebra $A \leq M_n(K)$ given by algebra generators unfortunately no mathematically rigorous efficient random generator is known which satisfies the requirement unless we have a K-linear generating system $b_1, \ldots, b_s$ of A and take a random linear combination of $b_1, \ldots, b_s$. Then the cost $R(A)$ is $O(sn^2)$. However, there are heuristic random generators (e.g., the one used in the Meataxe procedure [14] for finding composition series of modules over finite algebras) appear to work well in practice for similar problems.

We stress that our method is probabilistic of Monte Carlo type. By this we mean that the algorithm may fail or produce an incorrect output within a prescribed error probability ε. We note that there is a more restrictive (and more attractive) class of randomized algorithms, namely the Las Vegas algorithms which may still report failure but never produce incorrect answers.

In the analysis of the algorithms factors of magnitude $(\log n)^{O(1)}$ will be abbreviated by polylog n.

2. Preliminaries

In this section we give some definitions and basic facts concerning the structure of associative algebras. We assume that the reader is familiar with the basic standard notions associative algebras over fields (subalgebras, homomorphisms, ideals, factor algebras, modules, direct sums, tensor products, etc.). Throughout the paper K stands for a field. By an algebra we mean a finite dimensional associative algebra over K with identity denoted by 1_A or briefly by 1. Modules are assumed to be finite dimensional unital left A-modules. (The A-module U is called unital if $1_A u = u$ for every $u \in U$.) Let A be an algebra. For K-linear subspaces $B, C \subseteq A$ we denote by BC the K-linear span of $\{bc \mid b \in B,\ c \in C\}$. For $b, c \in A$ we denote by $[b,c]$ the additive commutator $bc-cb$ of b and c. We use the notation $[B,C]$ for the linear span of $\{[b,c] \mid b \in B,\ c \in C\}$. For a subset $B \subseteq A$ $C_A(B)$ stands for the centralizer of B in A: $C_A(B)=\{x \in A \mid [x,b]=0$ for every $b \in B\}$. The center $C_A(A)$ of A is denoted by $Z(A)$.

2.1. Structure of algebras

We encourage the reader familiar with the basic structure theory of algebras to skip this subsection.

We briefly recall Wedderburn's theorems on the structure of algebras. In every finite dimensional algebra A there exists a largest nilpotent ideal $Rad(A)$, called the radical of A. A is called semisimple if $Rad(A) = (0)$. The factor algebra $A/Rad(A)$ of an arbitrary algebra is semisimple. A is called simple if A admits no proper nonzero ideals. A semisimple algebra A can be decomposed into the direct sum of its minimal ideals $A_1, \ldots, A_r$. We refer to the simple algebras A_i as the simple components of A. A simple algebra A is isomorphic to $M_d(D)$ where D is a division algebra (or skew field) over A. By this we mean that D admits no zero divisors. If Z is a subfield of $Z(A)$ containing the identity of A then it is possible (and often convenient) to consider A as an algebra over Z. A is called central over K if $Z(A)=K$ (more precisely, $Z(A)=K1_A$). The dimension of a central simple K-algebra is always a square.

A module U over the semisimple algebra A can be decomposed as a direct sum of simple A-modules (modules with no proper nonzero submodules). If A is a simple algebra then there is only one isomorphism class of simple A-modules. By A^{op} we denote the algebra opposite to A. A^{op} has the same vector space structure as A but

the multiplication is reversed. A can be considered as an $A \otimes_K A^{op}$-module by the multiplication law $(a \otimes b)c = acb$. The ideal structure of A coincides with the $A \otimes_K A^{op}$-submodule structure of A. If A is a central simple K-algebra then $A \otimes_K A^{op} \cong M_{d^2}$ (where $d^2 = \dim_K A$) and every simple $A \otimes_K A^{op}$-module is isomorphic to A with the module structure given above (cf. [17], Corollary 12.3 and Proposition 12.4b).

2.2. Extending scalars

It is sometimes useful to consider the K'-algebra $K' \otimes_K A$ where K' is a field extension K. We refer to this construction as extending scalars. (For example if $A \leq M_n(K)$ is the matrix algebra generated by matrices $g_1, \ldots, g_m$ then we can think of $K' \otimes_K A$ as the subalgebra of $M_n(K')$ generated by the same matrices $g_1, \ldots, g_m$ considered as matrices over K'.) For a subspace B of A we consider $K' \otimes_K B$ embedded into $K' \otimes_K A$ in the natural way. Many constructions such as products and commutators of complexes and even centralizers behave well with respect to extension of scalars. For example, $[K' \otimes_K B, K' \otimes_K C] = K' \otimes_K [B, C]$ and $C_{K' \otimes_K A}(K' \otimes_K B) = K' \otimes_K C_A(B)$.

2.3. Separability and the Wedderburn–Malcev theorem

It is obvious that $K' \otimes_K Rad(A)$ is a nilpotent ideal of $K' \otimes_K A$. However, there are cases where $Rad(K' \otimes_K A)$ can be bigger than $K' \otimes_K Rad(A)$. A general sufficient condition for $Rad(K' \otimes_K A) = K' \otimes_K Rad(A)$ is that K' is a (not necessarily finite) separable extension of K. We say that A is separable over K if for every field extension K' of K the K'-algebra $K' \otimes_K A$ is semisimple. (Note that in [17], Chapter 10, a more general definition of separable algebras over an arbitrary ring is given. The simple definition given here for algebras over a field is equivalent to the general one, see [17], Corollary 10.6.) Separability of finite dimensional algebras generalizes the notion of separability of finite field extensions: by [17], Proposition 10.7, A is separable iff the centers of the simple components of A are separable extensions of K. From this characterization it follows immediately that A is separable over K if and only if $K' \otimes_K A$ is semisimple where K' denotes the algebraic closure of K. Obviously, over a perfect ground field K the notion of separability coincides with semisimplicity. It is immediate that if A is separable then $K' \otimes A$ is separable as well for an arbitrary field extension K' of K. Direct sums, homomorphic images and tensor products of separable algebras are separable as well (cf. [17], Section 10.5).

An extremely useful result where separability plays a role is the Wedderburn–Malcev Principal Theorem (See [17], Section 11.6. for a general form): Assume that $A/Rad(A)$ is separable. Then there exists a subalgebra $D \leq A$ such that $D \cong A/Rad(A)$ and $A = D + Rad(A)$ (direct sum of vector spaces). Furthermore, if D_1 is another subalgebra such that $D_1 \cong A/Rad(A)$ then there exists an element $w \in Rad(A)$ such that $D_1 = (1 + w)^{-1} D (1 + w)$.

We shall make use of the following consequence of the Principal Theorem.

Corollary 2. *Let A be a finite dimensional K-algebra and $B \leq A$ be a subalgebra of A which is separable over K and assume that $\widetilde{D}$ is a separable subalgebra of $A/Rad(A)$ containing B. Then there exists a subalgebra D of A such that $B \leq D$ and $D \cong \widetilde{D}$.*

Proof. Working in the pre-image of $\widetilde{D}$ at the natural projection $A \to A/Rad(A)$ we may assume that $\widetilde{D} = A/Rad(A)$. Then, by the first part of the principal theorem there exists a subalgebra $D_1 \leq A$ such that $D_1 \cong \widetilde{D}$ and $A = D_1 + Rad(A)$. Let π be the projection of A onto D_1 corresponding to this decomposition and $B_1 = \pi(B + Rad(A))$. By comparing dimensions it is clear that $B_1 + Rad(A) = B + Rad(A)$. By the second part of the principal theorem, applied to the algebra $B + Rad(A)$, there exists an element $w \in Rad(A)$ such that $(1 - w)^{-1}B(1 - w) = B_1$. Now the subalgebra $D = (1 - w)D_1(1 - w)^{-1}$ has the required property. □

2.4. Tori

As a matter of fact, the material of this subsection consists of an easy combination of known elementary facts. However, we are unable to propose a single textbook where all the facts we need in the subsequent part of the paper are stated. Therefore we formulate the less trivial facts in lemmas and give some hints to the proofs.

By a toral K-algebra or torus over K we mean a finite dimensional commutative K-algebra which is separable over K. Let K' stand for the algebraic closure of K. Then T is a torus if and only if $K' \otimes T$ is isomorphic to the direct sum of copies of K'. Let $T \leq M_n(K)$ be a commutative matrix algebra. Then T is a torus if and only if the matrices in T can be simultaneously diagonalized over K'. By this we mean that there exists a matrix $b \in M_n(K')$ such that $b^{-1}Tb \subseteq Diag_n(K')$, where $Diag_n(K')$ is the matrix algebra consisting of the diagonal n by n matrices. (The diagonalization can be obtained by decomposing $K' \otimes V$ into a direct sum of irreducible $K' \otimes T$-modules.)

Let A be a finite dimensional K-algebra with identity. By a maximal torus of A we mean a torus which is not properly contained in any other toral subalgebra of A. Let T_1 and T_2 be tori in A such that $T_1 \leq C_A(T_2)$. Then by [17], Proposition 10.5c, the subalgebra T generated by $T_1 \cup T_2$ is a torus as well. In particular, a commutative algebra contains a unique maximal torus. Furthermore, a maximal torus of A must contain the maximal torus of $Z(A)$. We call an element $a \in A$ semisimple (or separable) if a is contained in a torus $T \leq A$. This is equivalent to the subalgebra $K[a]$ generated by a and 1_A is a torus. As $K[a] \cong K[x]/f(x)$ where $f(x)$ is the minimal polynomial of a this is further equivalent to that $f(x)$ is a separable polynomial, i.e., $gcd(f(x), f'(x)) = 1$. Assume that A is a commutative algebra. Then the unique maximal torus in A consists of the semisimple elements of A. Hence if A is a field, then the maximal torus of A is the separable closure of K in A.

Lemma 3. *Let A be a finite dimensional K-algebra with identity and $T \leq A$ be a torus. Let $\phi : A \to Rad(A)$ stand for the natural projection. Assume further that A is a direct sum of ideals $A_1, \ldots, A_r$ and $Z \geq K1_A$ is a subfield of $Z(A)$. Then each of the*

following conditions are necessary and sufficient to that T is a maximal torus in A.

(1) *$\phi(T)$ is a maximal torus of $A/Rad(A)$.*

(2) *$T \cap A_i$ is a maximal torus of A_i for $i = 1, \ldots, r$.*

(3) *TZ, considered as a Z-algebra, is a maximal Z-torus of A and Z is a purely inseparable extension of $Z \cap T$.*

(4) *T is a maximal torus of its centralizer $C_A(T)$.*

Proof. We only give proofs that conditions (i) and (iii) are necessary and sufficient. The rest is easy and we leave the details to the reader. Assume that T is a maximal torus and $\widetilde{U}$ is a torus of $A/Rad(A)$ containing $\phi(T)$. Then by Corollary 2, there exists a subalgebra $U \leq A$ isomorphic to $\widetilde{U}$ which contains T. Since T is a maximal torus we have $U = T$ whence $\widetilde{U} = \phi(T)$. Thus condition (i) is necessary. Sufficiency of (i) is obvious.

Concerning condition (iii), let Z_0 be the separable closure of K in Z. Then Z_0 is the unique maximal K-torus of Z_0 and for every maximal K-torus T of A we have $Z \cap T = Z_0$. Let T be a K-torus of A containing Z_0 and let $T_1, \ldots, T_s$ be the simple components of T. Then the simple components of ZT are $ZT_1, \ldots, ZT_s$ and by [3], Proposition 2.5.13, each ZT_i is a purely inseparable field extension of T_i of degree $\dim_{Z_0} Z = \dim_K Z / \dim_K Z_0$ as well as a separable extension of the field $Z \cap ZT_i \cong Z$. It follows that ZT is a torus over Z and $\dim_K ZT / \dim_K T = \dim_K Z / \dim_K Z_0$, a ratio independent of T. From this it is immediate that if T is not a maximal K-torus then ZT is not a maximal Z-torus either.

To prove the reverse implication, let U be a Z-torus of A containing TZ and let $U_1, \ldots, U_t$ be the simple components of U. Then each U_i is a separable field extension of Z. Also, the unique maximal K-torus W of U is the sum of $W_1, \ldots, W_t$ where W_i is the separable closure of K in U_i. By [3] Proposition 2.5.13, $\dim_K U_i / \dim_K W_i = \dim_K Z / \dim_K Z_0$. This implies $\dim_K U / \dim_K W = \dim_K Z / \dim_K Z_0 = \dim_K ZT / \dim_K T$. Hence if T is maximal then $T = W$ and $\dim_K U = \dim_K ZT$ whence $U = ZT$ for every Z-torus U containing ZT. □

Lemma 4. *Assume that T is a maximal torus of A. Then $C_A(T)/Rad(C_A(T))$ is commutative.*

Proof. By Lemma 3, (i) and (iv), $T + Rad(C_A(T))$ is a maximal torus of $C_A(T)/Rad(C_A(T))$. Replacing A with $C_A(T)/Rad(C_A(T))$ we have to show that if A is semisimple and $T \leq Z(A)$ is a maximal torus of A then A is commutative. In view of Lemma 3, (ii), we may further assume that A is simple. Assume that A is not a division algebra. Then there exists an idempotent $e \in A$ such that $e \notin Z(A)$. The subalgebra B generated by T and e is a torus properly containing T (because $B \cong T[x]/(x^2 - x)$), a contradiction. It remains to eliminate the case when A is a noncommutative division algebra. Then by [17], Lemma 13.5, there exists a subfield $L \leq A$ which is a proper separable extension of $Z(A)$. Then the separable closure of K in L is a torus properly containing T, a contradiction. □

Lemma 5. *Assume that T is a maximal K-torus of A and K' be an arbitrary field extension of K. Then $K' \otimes_K T$ is a maximal K'-torus of $K' \otimes_K A$.*

Proof. Let $A' = K \otimes_K A$, $T' = K' \otimes_K T$, $H = C_A(T)$, and $H' = C_{A'}(T')$. It is obvious that $H' = K' \otimes_K H$. Let $I' = K' \otimes_K Rad(H)$. Then I' is a nilpotent ideal of H'.

We claim that it is sufficient to show that $T' + I'$ is a maximal torus in H'/I'. Indeed, if $U' \geq T'$ is a torus of A' then $U' + I'$ is a torus of H'/I' whence by the maximality of $T' + I'$ we have $U' + I' \leq T' + I'$. On the other hand $U' \cap I'$ is a nilpotent ideal of U' which must be zero as U' is separable. From this it is immediate that $U' \leq T'$.

By the claim we can work with $H/Rad(H)$ in place of H, i.e., we may assume that H is a commutative semisimple algebra. If $\operatorname{char} K = 0$ then $H = T$ and $H' = T'$ therefore the assertion is obvious. Assume that $\operatorname{char} K = p > 0$. Let $H_1, \ldots, H_r$ be the simple components of T. Then T is the sum of the separable closures of K is H_i. In particular, by [3], Corollary 2.5.14, T is the linear span over K of $\{a^{p^l} \mid a \in H\}$ where l is a sufficiently large integer. By the commutativity of H' the subalgebra T' is the linear span over K' of $\{a^{p^l} \mid a \in H'\}$. Assume that U' is a torus of H'. By Lemma 3, (ii) and again by [3], Corollary 2.5.14, $\{u^{p^l} \mid u \in U'\}$ span U' over K'. We obtained $U' \leq T'$. □

Lemma 6. *Assume that T is a maximal torus in a semisimple algebra A. Then $C_A(T) = TZ(A)$. Furthermore, if A is a central simple K-algebra then $\dim_K T = \sqrt{\dim_K A}$.*

Proof. We only give a proof of the first statement. The second assertion can be proved in a similar fashion. It is obvious that $C_A(T) \geq TZ(A)$. In view of Lemma 3, (ii) it is sufficient to give a proof of the statement in the special case where A is simple. Then $TZ(A)$, considered as a $Z(A)$-algebra is a maximal $Z(A)$-torus of A. Replacing K with $Z(A)$ we assume that A is a central simple K-algebra. Let K' be the algebraic closure of K. By Lemma 5, $T' = K' \otimes_K T$ is a maximal K'-torus in $A' = K' \otimes_K A$. Obviously $C'_A(T') = K' \otimes_K C_A(T)$. On the other hand, $A' \cong M_d(K)$ for some integer d. In $M_d(K)$ every maximal torus is conjugate to $Diag_d(K)$, the subalgebra of $d \times d$ diagonal matrices and it is straightforward to verify the assertion for $Diag_d(K)$. □

2.5. Centralizers of tori and Fitting decompositions

Let T be a torus over K with $d = \dim_K T$. We recall some facts from [17], Section 10.2, specialized to the context of tori. Let T be a torus over K. The map $\mu : T \otimes_K T \to T$ given by the law $\mu(a \otimes b) = ab$ is a K-algebra epimorphism. The kernel of μ is the ideal of $T \otimes_K T$ generated by the elements $b \otimes 1 - 1 \otimes b$ where b runs over T (or, equivalently, on a basis of T). Let $I = \{u \in T \mid a \ker \mu = 0\}$ be the ideal of $T \otimes_K T$ complementary to $\ker \mu$. Then $T \otimes_K T = I \oplus \ker \mu$ and the restriction of μ establishes an algebra isomorphism $I \cong T$. Let Φ_T stand for the identity element of I. Note that

Φ_T is characterized by the properties $\mu(\Phi_T)=1$ and $(1\otimes b)\Phi_T=(b\otimes 1)\Phi_T$ for every $b\in T$. (We remark that this is the definition of a separating idempotent. Separating idempotent exists for an arbitrary separable algebra. However, in the noncommutative case it is not necessarily unique.)

Let U be a $T\otimes_K T$-module. Then for every $u\in U$ we have $u=\Phi_T u+(1-\Phi_T)u$. This gives rise to a decomposition of U as the direct sum of submodules $U_0=IU=\Phi_T U$ and $U_1=(\ker\mu)U=(1-\Phi_T)U$. Then Φ_T and $1-\Phi_T$ act as the projections of U to U_0 and U_1 with respect to the decomposition $U=U_0\oplus U_1$. We have $U_0=\{u\in U\,|\,(\ker\mu)U=(0)\}=\{u\in U\,|\,(b\otimes 1-1\otimes b)u=0 \text{ for every } b\in T\}$ and $U_1=(\ker\mu)U=\{b\otimes 1-1\otimes b\,|\,b\in T\}(T\otimes_K T)U=\{b\otimes 1-1\otimes b\,|\,b\in T\}U$. We refer to U_0 as the Fitting null component and to U_1 as the Fitting one component. This terminology is justified by the following. The adjoint action of $b\in T$ on U is defined as the linear transformation $\operatorname{ad} b: u\mapsto (b\otimes 1-1\otimes b)u$. This gives rise to a representation of T considered as an abelian (and hence nilpotent) Lie algebra and the decomposition $U=U_0+U_1$ appears to be the same as the Fitting decomposition of U given in [7], Theorem II.4.

Now assume that the torus T is a subalgebra of the algebra A. We consider A as a $T\otimes_K T$-module in the natural way (multiplication from both sides). Then the Fitting null component A_0 is $\{a\in A\,|\,(b\otimes 1-1\otimes b)a=[b,a]=0 \text{ for every } b\in T\}=C_A(T)$ while the Fitting one component A_1 is the linear span of the elements of the form $(b\otimes 1-1\otimes b)a=[b,a]$ $(a\in A, b\in T)$. Thus $A=C_A(T)+[T,A]$, a direct sum of vector spaces and the projections of A corresponding to this decomposition are Φ_T and the map $a\mapsto a-\Phi_T(a)$.

Similarly, let U and W be T-modules. For convenience we consider U and W as right T-modules. For $u\in U$, $c\in Hom_K(U,V)$ and $a,b\in T$ let $((a\otimes b)c)u:=acbu$. The linear extension of this rule to $T\otimes T$ makes $Hom_K(U,V)$ a $T\otimes T$-module. Then the Fitting null component of $Hom_K(U,V)$ is $Hom_T(U,V)$.

We also need an explicit representation of Φ_T in terms of rank one tensors. This appears to be extremely useful for computational purposes. We use a construction which can be generalized to the more general context of Frobenius algebras, cf. [6], Theorem 62.11. For an application in computational group theory we refer the reader to [2,11]. Since the formulations appearing in the literature are slightly different from that we need we give some hints to a an easy proof of correctness of the construction in the special case of tori.

For $a\in T$ let $Tr(a)$ stand for the trace of the linear transformation of T given as $b\mapsto ab$. By [3], Proposition 3.8.7, separability of T implies that the linear function $Tr: T\to K$ is not identically zero. As a consequence, the bilinear trace form $(,)$ on T given as $(a,b)=Tr(ab)$ is a non-degenerate bilinear form on T. Let $b_1,\ldots,b_d$ be an arbitrary basis of T and $b'_1,\ldots,b'_d$ be the dual basis with respect to the form $(,)$. We claim that

$$\Phi_T=\sum_{i=1}^{d} b_i\otimes b'_i. \tag{1}$$

To see this we note first that it is straightforward to verify that the element $f = \sum_{i=1}^{d} b_i \otimes b_i' \in T \otimes_K T$ does not depend on the particular choice of the basis $b_1, \ldots, b_d$. Let K' be the algebraic closure of K and $T' = K' \otimes_K T$. We think of T as embedded in T' in the natural way. It is obvious that Φ_T satisfies the conditions for $\Phi_{T'}$, and hence $\Phi_{T'} = \Phi_T$. On the other hand, we know that T' is isomorphic to the direct sum of d copies of K'. Let $e_1, \ldots, e_d$ be the identity elements of the simple components of T'. Then $e_1, \ldots, e_d$ form a self-dual basis of T' with respect to the bilinear trace form and hence $f = \sum_{i=1}^{d} e_i \otimes e_i$. One easily verifies that $\sum_{i=1}^{d} e_i \otimes e_i$ also satisfies the properties characterizing $\Phi_{T'}$. Thus $\Phi_T = \Phi_{T'} = \sum_{i=1}^{d} e_i \otimes e_i = f$.

3. Decomposition with respect to a maximal torus

In this section we develop a structure theory which serves as a theoretical foundation for the subsequent algorithms. First we fix some notation. Let K be an arbitrary field. We denote by ϕ the natural projection $A \to A/Rad(A)$. Let $\widetilde{C}$ be the set of those central elements of $A/Rad(A)$ which are separable over K. Obviously, $\widetilde{C}$ is the unique maximal torus of $Z(A/Rad(A))$. Let T be a fixed maximal torus of A and let the set $C \subseteq T$ consist of those elements of T which are central modulo the radical:

$$C = \{x \in T \mid \phi(x) \in Z(A/Rad(A))\}.$$

C is a subalgebra of T as C is the intersection of T and the subalgebra $\phi^{-1}Z(A/Rad(A))$. By Lemma 3, $\phi(T)$ is a maximal torus of $A/Rad(A)$ and hence $\phi(C) = \phi(T) \cap Z(A/Rad(A)) = \widetilde{C}$.

In view of Section 2.5

$$A = S + N, \tag{2}$$

where $S = C_A(C)$ and $N = [C, A]$. We remark that, by Wedderburn–Malcev, applied to the algebra $\phi^{-1}(\widetilde{C})$, the subalgebra C is determined up to conjugation by a unit in A. Therefore the structural properties of S and N are independent of the particular choice of T.

Proposition 7. *N is an S-invariant subspace of $Rad(A)$, i.e., $SN \subseteq N$, $NS \subseteq N$, and $N \subseteq Rad(A)$,*

Proof. The inclusions $SN \subseteq N$ and $NS \subseteq N$ follow from $s[x, y] = sxy - syx = xsy - syx = [x, sy]$ and $[x, y]s = xys - yxs = xys - ysx = [x, ys]$, respectively ($s \in S, x \in C, y \in A$). To prove the remaining inclusion, observe that $\phi(C) = \widetilde{C}$ is in the center of $A/Rad(A)$. From this we immediately obtain that $\phi(N) = [\phi(C), \phi(A)] = (0)$, whence $N \subseteq Rad(A)$. □

The radical inherits the decomposition (2) of A in the following sense.

Proposition 8. $Rad(A) = Rad(S) + N$.

Proof. $ARad(S)=(S+N)Rad(S)=Rad(S)+NRad(S)\subseteq Rad(S)+N\subseteq Rad(S)+Rad(A)$, hence as is nilpotent for every $a\in A$ and $s\in Rad(S)$. This implies the inclusion $Rad(S)+N\subseteq Rad(A)$. To prove the reverse inclusion let $a\in Rad(A)$. Then $a=s+n$ for some $s\in S$ and $n\in N$. We have $s=a-n\in (Rad(A)+N)\cap S=Rad(A)\cap S\subseteq Rad(S)$, whence $a\in Rad(S)+N$. □

The subalgebra S admits a decomposition which generalizes the Wedderburn decomposition of semi-simple algebras.

Proposition 9. *Let $C_1,\dots,C_r$ be the simple components of C. Then S is the direct sum $S=S_1+\cdots+S_r$ of ideals $S_1=C_1S,\dots,S_r=C_rS$. For every $i\in\{1,\dots,r\}$ the factor algebra $S_i/Rad(S_i)$ is a simple algebra. Furthermore, if we consider S_i as a C_i-algebra in the natural way then $Z(S_i/Rad(S_i))$ is a purely inseparable extension of C_i.*

Proof. The first two statements are proved in [15], Theorem 49.1. To see the last assertion, let $Z_1,\dots,Z_s$ be the simple components of $S/Rad(S)$. Then the simple components of $\phi(C)$, the image of C at the the natural projection $\phi: S\to Rad(S)$, are $Z_i\cap\phi(C)$. It follows that (after re-indexing) $Z_i\cap\phi(C)=\phi(C_i)$. Hence $\phi(C_i)S=\phi(C_iS)=Z_i\phi(S)$. Since $Z_i\phi(S)$ are the simple components of $S/Rad(S)$ we obtained that $S_i/Rad(S_i)\cong\phi(S_i)$ are simple. Also, as $\phi(C_i)$ is the set of elements of Z_i which are separable over K, $Z_i=Z(Z_i\phi(S))$ is purely inseparable over $\phi(C_i)$. □

An algebra B such that $B/Rad(B)$ is simple is called primary. We shall refer to the decomposition of S given in Proposition 9 as the primary decomposition of S and to the ideals $S_1,\dots,S_r$ as the primary components of S.

Let $H=C_A(T)$, the centralizer of T. Obviously, H is a subalgebra of S. We remark that, by [21], Thm. 4.4.8, H is a Cartan subalgebra of A (considered as a Lie algebra).

Theorem 10. *Keeping the notation introduced above, $Rad(S)$ is the ideal of S generated by $Rad(H):Rad(S)=S\,Rad(H)S$. Furthermore, every nilpotent element of H is in $Rad(H)$.*

Proof. It is clearly sufficient to prove the assertions for the primary components of S separately. Therefore we assume that S is primary, i.e., C is a field. We can further consider S as a C-algebra rather than as a K-algebra. Thus it is sufficient to consider an algebra S where $\widetilde{Z}=Z(S/Rad(S))$ is a purely inseparable field extension of K.

First we show that every nilpotent element of H is in the radical of S. To see this, let h be an arbitrary nilpotent element of H. Let $\widetilde{T}$ denote the image of T at the natural projection $\phi: S\to S/Rad(S)$. By Lemma 3, (i), $\widetilde{T}$ is a maximal torus of $S/Rad(S)$. Consider the centralizer $\widetilde{U}$ of the algebra $\widetilde{T}$ in $S/Rad(S)$. Obviously $\phi(h)$ is a nilpotent element of $\widetilde{U}$. By Lemma 6, $\widetilde{U}=\widetilde{T}Z(S/Rad(S))$, a commutative semisimple algebra. Since in a commutative algebra every nilpotent element is in the

radical, $\phi(h) \in Rad(\widetilde{U}) = (0)$. This implies the last statement of the theorem together with the inclusion $Rad(H) \subseteq Rad(S)$. From this $S\,Rad(H)S \subseteq Rad(S)$ is immediate.

To prove the reverse inclusion, let K' be the separable algebraic closure of K, $S' = K' \otimes_K S$, $T' = K' \otimes_K T$, and $H' = K' \otimes_K H$. Then, by Lemma 5, T' is a maximal torus in the K'-algebra S' and H' is the centralizer of T' in S'. Let $I' = K' \otimes_K Rad(A)$. Then $K' \otimes_K Rad(H) = I' \cap H' = C_{I'}(T')$. Since K' is a separable extension of K, $Rad(S') = K' \otimes_K Rad(S)$ and $Rad(H') = K' \otimes_K Rad(H)$, therefore we are done if we prove that $Rad(S') = S'Rad(H)S'$. In order to simplify notation, we replace K with K', S with S', etc.

Let $\widetilde{T}$ denote the image of T at the natural projection $\phi : S \to S/Rad(S)$. The algebra $S/Rad(S)$ is a central simple $\widetilde{Z}$-algebra. By [17], Theorem 13.5, there exists a finite separable field extension L of Z such that $L \otimes_Z S/Rad(S) \cong M_d(L)$ for some integer d. Since $\widetilde{Z}$ is a purely inseparable extension of K which is closed under finite separable extensions, so is $\widetilde{Z}$ and hence $L = Z$. This implies $S/Rad(S) \cong M_d(\widetilde{Z})$. Obviously $\widetilde{T}\widetilde{Z}$ is a torus of $S/Rad(S)$. Since the minimal polynomial of every element of $\widetilde{T}\widetilde{Z}$ splits into linear factors over $\widetilde{Z}$, by [21], Proposition 1.4.4, $\widetilde{T}\widetilde{Z}$ considered as a subalgebra of $M_d(\widetilde{Z})$ is conjugate in $M_d(\widetilde{Z})$ to a subalgebra of $Diag_d(\widetilde{Z})$. In other words, there exists a $\widetilde{Z}$-algebra isomorphism $\psi : S/Rad(S) \cong M_d(\widetilde{Z})$ such that $\psi(\widetilde{T}\widetilde{Z}) \leq Diag_d(\widetilde{Z})$. Since $\psi(\widetilde{T})$ is the set of elements of $\psi(\widetilde{T}\widetilde{Z})$ which are separable over K, we have $\psi(\widetilde{T}) \leq Diag_d(K)$, the subalgebra of $M_d(\widetilde{Z})$ of diagonal matrices with entries from K. In particular, $\psi(\widetilde{T}) \leq M_d(K)$. On the right hand side of the inclusion stands a central simple K-subalgebra of $M_d(\widetilde{Z})$. Then $\widetilde{D} = \psi^{-1}M_d(K)$ is a central simple (and hence separable) K-subalgebra of $S/Rad(S)$ containing $\widetilde{T}$ as a maximal torus. Corollary 2 implies the existence of a central simple K-subalgebra D of S containing T.

We are going to show the equality $Rad(S) = DRad(H)D$. To this end we consider $Rad(S)$ as a module over $D \otimes_K D^{op}$, where D^{op} is the algebra opposite to D. By [17], Proposition 12.4b, $D \otimes_K D^{op} \cong M_{d^2}(K)$ ($d = \dim_K T$), which is a simple algebra. In particular, every simple $D \otimes_K D^{op}$-module is isomorphic to the module D with multiplication law $(d_1 \otimes d_2)v = d_1 v d_2$ (cf. [20], Corollary 12.3). Obviously, this module is generated by the identity element 1_D of D which belongs to the subspace $\{v \in D \mid (1 \otimes a)v = (a \otimes 1)v$ for every $a \in D\} = Z(D)$. Now $Rad(S)$, being a unital $D \otimes_K D^{op}$-module, can be decomposed into a direct sum of simple modules. The preceding observation, applied to the simple components, implies that $Rad(S)$ is generated by the subspace $\{v \in Rad(S) \mid (1 \otimes a)v = (a \otimes 1)v$ for every $a \in D\} = \{v \in Rad(S) \mid va = av$ for every $a \in D\} = C_{Rad(S)}(D) \leq C_{Rad(S)}(T) = Rad(H)$. This concludes the proof of the theorem. □

We shall make use of the following characterization of C which will enable us to compute C without calculating $Rad(A)$ first.

Theorem 11. *Set $L = [A,A] \cap T$. Then L is a linear subspace of T and $C = \{x \in T \mid xL \subseteq L\}$.*

Proof. It is obvious that L is a linear subspace of T. Let $C_1 = \{x \in T \mid xL \subseteq L\}$. The inclusion $C \subseteq C_1$ follows easily from $C[A,A] = [CA,A] = [A,A]$. We have to show that $\dim_K C_1 \leq \dim_K C$.

We claim that $L = ([A,A] + Rad(A)) \cap T$. The inclusion $L \subseteq ([A,A] + Rad(A)) \cap T$ is obvious. To prove the reverse inclusion, let K' be the algebraic closure of K, $A' = K' \otimes_K A$, $T' = K' \otimes_K A$, and $L' = K' \otimes_K L$. Obviously $[A',A'] = K' \otimes_L [A,A]$ and hence $L' = [A',A'] \cap T'$. We have to show that $L' \supseteq [A',A'] + K' \otimes_K Rad(A) \cap T'$. In view of $K' \otimes_K Rad(A') \supseteq Rad(A')$ it is sufficient to establish the inclusion $L' \supseteq ([A',A'] + Rad(A')) \cap T'$. Since T' is a torus in A' and K' is perfect, by Corollary 2 there exists a subalgebra D' which contains T' and is isomorphic to $A'/Rad(A')$. Obviously $[A',A'] + Rad(A') = [D',D'] + Rad(A')$. From $D \cap Rad(A) = (0)$ and $[D',D'] \subseteq D'$ we infer that $D \cap [A',A'] + Rad(A') = [D',D']$. As $T' \leq D'$ we have $T' \cap ([A',A'] + Rad(A')) = [D',D'] \cap T' \subseteq [A',A'] \cap T' = L'$.

By the claim it is sufficient to verify the assertion modulo $Rad(A)$. Furthermore, we can work separately in the simple components of $A/Rad(A)$. Thus for the rest of the proof we may assume that A is a simple algebra. Then $Z = Z(A)$ is a purely inseparable extension of C. As $C_1 = ZT \cap T$ and $C = Z \cap T$ it is sufficient to establish the inequality $\dim_K ZC_1 \leq \dim_K Z$. Observe that $ZC_1 \subseteq \{x \in ZT \mid xZL \subseteq ZL\}$ and $ZL = [A,A] \cap ZT$. Consider A as a central simple algebra over Z. Then ZT is a maximal Z-torus in A and it is sufficient to show that $\dim_Z \{x \in ZT \mid xZL \subseteq ZL\} \leq 1$. In order to simplify notation, we write K in place of Z, T in place of ZT and ZL in place of L. Then it remains to prove $\dim_K C_1 \leq 1$ in the special case where A is a central simple algebra over K. It is also clear that we may assume that K is algebraically closed.

Then we can identify A with the full matrix algebra $M_d(K)$ where $d = \dim_K T$ and T can be identified with $Diag_d(K)$, the algebra of diagonal matrices. For an arbitrary element $x \in A$ let $\mathrm{Tr}(x)$ stand for the trace of x as a d by d matrix. It is well known that $[A,A] = \{x \in A \mid \mathrm{Tr}(x) = 0\}$ even if the characteristic is positive. (Both subspaces have codimension one.) From this fact we infer $L = \{x \in T \mid \mathrm{Tr}(x) = 0\}$. Observe that the bilinear form $\langle x, y \rangle = \mathrm{Tr}(xy)$ is non-degenerate on T. The preceding characterization of L implies that C_1 is the orthocomplement of L in T with respect to the bilinear trace form, therefore $\dim C_1 = 1$, concluding the proof of the theorem. □

4. A reduction to the commutative case

We assume that the algebra $A \leq M_n(K)$ is given by generators. By this we mean that the input consists of matrices $g_1, \ldots, g_m \in M_n(K)$ and A is the enveloping algebra of $g_1, \ldots, g_m$ and the identity matrix. The output is expected to be an array $a_1, \ldots, a_t$ of matrices from $Rad(A)$ such that the ideal of A generated by $a_1, \ldots, a_t$ is $Rad(A)$.

Theorem 12. *There is an algorithm which reduces the problem of computing the radical of A to the problem of calculating the radical of a commutative algebra B which is a factor of a subalgebra of A. The algorithm performs $n^{O(1)}$ operations in K.*

Proof. We can calculate a basis $b_1,\dots,b_s$ of A by a straightforward method with $n^{O(1)}$ operations in K. Then we find a K-basis $u_1,\dots,u_d$ of a maximal torus T of A using the method of [8] at cost $n^{O(1)}$ operations. We use the notation of Section 3. Calculation of a K-basis of the centralizer $H = C_A(T)$ can be accomplished by solving the system of homogeneous linear equations $xu_i - u_i x = 0$ $(i = 1,\dots,d)$ in A.

We find the subalgebra C using the characterization given in Theorem 11. We select a linear basis of the subspace $[A,A]$ from the commutators $[b_i,b_j]$ $(i,j = 1,\dots,s)$ and calculate a basis of the intersection $L = T \cap [A,A]$ and then a basis $c_1,\dots,c_k$ of the stabilizer $C = \{x \in T \mid xL \subseteq L\}$. Both tasks can be accomplished with $n^{O(1)}$ operations by solving systems of linear equations. We omit the details.

Now a basis of N can be selected from the commutators $[b_i,c_j]$ $(i = 1,\dots,t,\ j = 1,\dots,s)$. We can select a basis of the ideal $I = H[H,H]H$ in a similar way. Also, we can find a basis of the factor algebra $H_1 = H/I$ together with the multiplication table of H/I with respect to that basis. By Lemma 4 $H/Rad(H)$ is commutative, therefore $I \leq Rad(H)$ and hence H_1 is a commutative algebra. We pass the multiplication table of H_1 to the oracle for finding the radical of commutative algebras. Then $Rad(H)$ is generated by a basis of $[H,H]$ and a system of representatives of the generators of H_1. These together with the basis of N generate $Rad(A)$ as an ideal of A by Proposition 8 and Theorem 10. □

We briefly comment on the significance of Theorem 12. It is known (see [5,20]) that in characteristic $p > 0$ the radical of an algebra cannot be calculated by an algorithm using merely the field operations in K. Therefore only a reduction to an algorithmically unsolvable problem can be expected. In [5] an algorithm for computing $Rad(A)$ is given which makes several calls to an oracle for solving systems of semilinear equations of the form $\alpha_1 x_1^p + \cdots + \alpha_k x_k^p = 0$, where $k \leq \dim_K A$. It was also pointed out that solving such a system can be reduced to finding the radical of a commutative algebra of dimension p^k. The result of this section is a reduction to a *single instance* of finding the radical of a commutative algebra B of dimension at most $\dim_K A$. We remark that a nilpotent ideal J of B together with a presentation of B/J in terms of $s = O(\log_p \dim_K B)$ generators can be calculated in a rather straightforward way. (The technical details appear to be too complicated to include here.) Therefore computing $Rad(B)$ can be reduced to calculating the radical of an ideal in the polynomial ring $K[x_1,\dots,x_s]$.

5. Computing Fitting decomposition with respect to a semisimple matrix

Let $u \in M_m(K)$ be a semisimple matrix and T be the torus generated by a and the identity matrix. Let Φ_T stand for the element of $T \otimes_K T$ given in Section 2.5. Our aim is to calculate $\Phi_T a$ efficiently for an arbitrary matrix $a \in M_n(K)$. We know that $T \cong K[x]/(f(x))$ where $f(x)$ is the minimal polynomial of u. Let $V = K^n$, the vector spaces of column vectors of length n over K. We consider V as a T-module or, equivalently, as a $K[x]$-module. Then $C_{M_n(K)}(T) \cong End_T(V) \cong End_{K(x)}(V)$.

We presume that we have found a decomposition of V as a direct sum of cyclic T-submodules $V_1,\dots,V_t$ such that for any pair V_i,V_j of components either $V_i \cong V_j$ as T-modules or $Hom_T(V_j,V_j)=(0)$. Then $End_K(V)=\oplus\sum_{i,j} Hom_K(V_i,V_j)$ and for $a=\sum_{i,j} a_{ij}$ where $a_{ij}\in Hom_K(V_i,V_j)$ we have $\Phi_T a=\sum_{i,j}\Phi_T a_{ij}$. For non-isomorphic V_i,V_j we know that $Hom_K(V_i,V_j)=(0)$ therefore Φ_T is zero on $Hom_K(V_i,V_j)$. For isomorphic V_i and V_j we identify V_i and V_j using a T-module isomorphism.

The main task is computing Φ_T on a cyclic T-module W. Let $d=\dim_K W$. We may assume that T acts faithfully on W. Indeed, if I is an ideal of T such that $IW=(0)$ then $\Phi_{T/I}$ and Φ_T coincide on $End_K(W)$. We identify T with a subalgebra of $End_K(W)$. A faithful cyclic T-module is isomorphic to the regular module $T\cong K[x]/(g(x))$ where $g(x)$ is the minimal polynomial of the generator u on W. These isomorphisms (provided that we constructed it effectively) will allow us to perform a multiplication in T as well as multiplication of a vector and a matrix from T with $O(d\,\mathrm{polylog}\,d)$ operations in K using polynomial arithmetic modulo $g(x)$ (cf. [4], Section 1.3). The isomorphisms are assumed to be given as follows. Let w be a vector which generates W as a T-module. We work in the basis $w_i=u^i w$ $(i=0,\dots,d-1)$ of W. Note that in this basis the coefficients of $g(x)$ can be read from the last column of the matrix of u. In T we use the basis $1,u,\dots,u^{d-1}$. If we have an element $a\in T$ represented as a matrix in terms of the basis $w_0,\dots,w_{d-1}$ then the coordinates of a with respect to the basis $1,\dots,u^{d-1}$ can be read from the vector aw_0 which is the first column of the matrix. Conversely, if a is given as $\sum_i \alpha_i u^i$ then the columns of the matrix of a are the vectors aw_i. Hence the matrix of a can be calculated at total cost $O(d^2\,\mathrm{polylog}\,d)$.

From $\dim_K W=\dim_K T$ we infer $End_T(W)=T$. (This can be seen by noting that over the algebraic closure of K the torus T is conjugate to the algebra of the diagonal matrices.) Hence we know that $\Phi_T a\in T$ for every element $a\in End_T(W)$. In view of the preceding discussion we have to show how to calculate $\Phi_T a w_0$ efficiently. In view of formula (1), we have $\Phi_T a=\sum_{i=0}^{d-1} u_i' a u^i$ where u_i' is the basis of T dual with respect to the trace form. Representation of u_i' in terms of $1,\dots,u^{d-1}$ can be obtained as the rows of the inverse of the matrix $(Tr(u^i u^j))_{i,j=0}^{d-1}$. The matrix $(Tr(u^i u^j))_{i,j=0}^{d-1}$ and its inverse can be calculated using $O(d^2\,\mathrm{polylog}\,d)$ operations using the method described as a part of [4], Algorithm 2.6.1. Observe that $au^i w_0=aw_i$, which is the ith column of the matrix of a. Then for every $i\in\{0,\dots,d-1\}$ the vector $u_i' a u_i w_0$ can be calculated with $O(d\,\mathrm{polylog}\,d)$ operations using polynomial arithmetic modulo $g(x)$. The total cost of computing $\Phi_T a$ (on a cyclic module with the presumed basis) is therefore $O(d^2\,\mathrm{polylog}\,d)$.

We return to determining $\Phi_T a$ on the whole V. Assume that we have a basis $v_{11},\dots,v_{1d_1},\dots,v_{t1},\dots,v_{dt}$ such that the subspaces V_i spanned by $v_{i1},\dots,v_{id_j}$ are cyclic T-submodules such that V_i and V_j are either isomorphic T-modules or $Hom_T(V_i,V_j)=(0)$ $(i,j=1,\dots,t)$ and the basis given on V_i is of the form $v_{ik}=u^{k-1}v_{i1}$ $(i=1,\dots,t,\ k=1,\dots,d_i)$. Then for every matrix $a\in M_n(K)$ writing a in terms of the new basis (i.e. conjugating a by the basis transition matrix) can be accomplished with $O(MM(n))$ operations. Then we calculate $\Phi_T a$ block-wise. The total cost of this amounts to

$O(n^2 \operatorname{polylog} n) = O(MM(n)\operatorname{polylog} n)$ operations. Writing the result back in terms of the standard basis of V requires further $O(MM(n))$ operations.

It remains to show how to find a basis with the required properties. We follow the method of Giesbrecht for calculating the rational Jordan form, cf. [13]. However, here we are not allowed to factor the minimal polynomial. Recall that the companion matrix $Comp(g(x))$ of a monic polynomial $g(x) \in K[x]$ of degree d is the matrix of the action of x on the $K[x]$-module $K[x]/(g(x))$. For every matrix $u \in M_n(K)$ there exists a unique block diagonal matrix $Frob(u)$ similar to u which is composed from the companion matrices of polynomials $f_1(x), \ldots, f_s(x) \in K[x]$ satisfying $f_s(x) \mid f_{s-1}(x) \mid \cdots \mid f_1(x)$. The polynomials $f_1(x), \ldots, f_s(x)$ are called the invariant factors of u and the matrix $Frob(u)$ is called the Frobenius form of u. Obviously $f_1(x)$ is the minimal polynomial of u and $f_1(x) \cdots f_s(x)$ is the characteristic polynomial of u. The Frobenius form $Frob(u)$ together with a matrix $b' \in GL_n(K)$ such that $b'^{-1} u b' = Frob(u)$ can be computed with $O(MM(n)\operatorname{polylog} n)$ operations in K using the Las Vegas algorithm of Giesbrecht [13]. Let $f_1(x), \ldots, f_s(x)$ be the invariant factors of U. Set $f_{s+1}(x) = 1$ and let $g_1(x), \ldots, g_r(x)$ be the collection of non-constant quotients of the form $f_i(x)/f_{i+1}(x)$ $(i = 1, \ldots, s)$. In our case where u is semisimple and therefore $f_1(x)$ is square-free we have $f_1(x) = g_1(x) \cdots g_r(x)$. Furthermore, it is easy to see that u is similar to the block diagonal matrix u' composed of s_1 companion matrices of $f_1(x)$, s_2 companion matrices of $f_2(x)$, and so on. The multiplicities s_i are determined by $\prod_{i=1}^{s} f_i(x) = \prod_{i=1}^{r} g_i(x)^{s_i}$. Since u' is similar to u, we have $Frob(u') = Frob(u)$ and, again by the method of Giesbrecht, we can calculate a matrix $b'' \in GL_n(K)$ such that $b''^{-1} u' b'' = Frob(u)$. With $b = b' b''^{-1}$ we have $u' = b^{-1} u b$. Now the columns of the matrix b form a basis with the required properties. The total cost amounts to $O(MM(n)\operatorname{polylog} n)$ operations. We have proved the following.

Proposition 13. *Let $u \in M_n(K)$ be a semisimple matrix and let T be the matrix algebra generated by u and the identity matrix. Let $a \in M_n(K)$ be an arbitrary matrix. Then $\Phi_T a$ can be calculated by a Las Vegas algorithm using $O(MM(n)\operatorname{polylog} n)$ operations in K.*

6. A Monte Carlo method for finding the radical

In this section we assume that K is a sufficiently large perfect field together with an efficient method for finding the square-free part of polynomials of degree n with $SF_K(n)$ operations.

Throughout this section K' stands for an algebraic closure of K and $A' = K' \otimes_K A$. We think of A as embedded into A'. The input is the same as described in Section 4. We assume that random elements of A are generated independently according to a distribution satisfying condition $AlgRand(A, n^2, \delta)$ defined in the introduction. The cost of selecting a single random element of A is denoted by $R(A)$. The algorithm follows

the lines of the method described in Section 4. We describe the main ingredients using the notation of Section 3.

6.1. Jordan decomposition

Let $u \in M_n(K)$ be a matrix. Since K is perfect, there exists a semisimple matrix $u_s \in M_n(K)$ and a nilpotent matrix $u_n \in M_n(K)$ such that $[u_s, u_n] = 0$ and $u = u_s + u_n$ (cf. [21], Propositions 1.4.6 and 1.4.10). Furthermore, u_s and u_n are unique with these properties and both belong to the matrix algebra generated by u. The decomposition $u = u_s + u_n$ is referred to as the Jordan decomposition of u. The matrices u_s and u_n are called the semisimple respectively the nilpotent part of u. In this paper it will be more convenient to denote u_s by $J_s(u)$ and u_n by $J_n(u)$. In [1] a method based on the Newton–Hensel lifting procedure is presented which calculates a polynomial $s(x) \in K[x]$ of degree less than n from the square-free part of the minimal polynomial of u such that $s(u) = J_s(u)$. Combining this with Giesbrecht's Las Vegas methods [13] for calculating the minimal polynomial and for evaluating $s(u)$ we can compute $J_s(u)$ with $O(MM(n)\text{polylog}\, n + SF_K(n))$ operations.

6.2. Finding a maximal torus

We show that the semisimple part of a random element generates a maximal torus with a good chance. The argument used here is a simplified (and improved) version of a proof given by Eberly and Giesbrecht [10] for a special case.

Lemma 14. *Let d stand for the dimension of a maximal torus in A'. There exists a polynomial function $f : A' \to K'$ of degree $d^2 - d$ such that for $u \in A'$ the subalgebra T' generated by the semisimple part $J_s(u)$ of u and the identity matrix is a maximal torus of A' if and only if $f(u) \neq 0$.*

Proof. By Wedderburn's theorem $A'/Rad(A) \cong \oplus_{i=1}^{s} M_{n_i}(K')$. A maximal torus in $M_{n_i}(K')$ is conjugated to the set of diagonal matrices. It follows that $d = \sum_{i=1}^{s} n_i$. We assume that $\oplus_{i=1}^{s} M_{n_i}(K')$ is embedded into $M_d(K')$ in the natural way. Let $\phi : A' \to M_d(K')$ be the composition of the natural projection $A' \to A'/Rad(A')$ with this embedding. Observe that ϕ commutes with taking the semisimple part: $\phi(J_s(u)) = J_s(\phi(u))$ for every $u \in A'$. We claim that the torus T generated by the identity of A and semisimple part $J_s(u)$ of u has dimension d if and only if $\phi(u)$ has d distinct eigenvalues. Indeed, since $\ker \phi = Rad(A')$ and $T \cap Rad(A') = (0)$, T and $\phi(T)$ are isomorphic. On the other hand, $\phi(T)$ is generated by $\phi(J_s(u)) = J_s(\phi(u))$ and the identity, hence the dimension of $\phi(T)$ is the degree of the minimal polynomial of $J_s(\phi(u))$ which equals the number of distinct eigenvalues of $\phi(u)$.

Let $\chi_u(x)$ denote the characteristic polynomial of the adjoint action $\text{ad}\,\phi(u) : w \mapsto \phi(u)w - w\phi(u)$ of $\phi(u)$ on $M_d(K')$. We claim that the nullity of $\text{ad}\,\phi(u)$ is at least d and equality holds if and only if $\phi(u)$ has d distinct eigenvalues. Indeed, we may assume

that $\phi(u)$ is of Jordan normal form. One easily verifies that $\operatorname{ad}\phi(u)$ acts nilpotently on the block diagonal matrices whose blocks correspond to the Jordan blocks of $\phi(u)$. This implies the inequality and the "only if" part of the claim concerning the equality. The "if" part is even easier.

It follows that $\phi(u)$ has d eigenvalues if and only if the coefficient c_u of the term x^d in $\chi_u(x)$ is zero. Let $f(u)$ stand for this coefficient. It is known that the coefficient of x^l in the characteristic polynomial of a linear transformation on a vector space W is a homogeneous polynomial function on $End(W)$ of degree $\dim W - l$. In our case $\dim W = d^2$ and $l = d$. Our function f being the composition of a homogeneous polynomial function of degree $d^2 - d$ and the linear maps ad and ϕ is either zero or homogeneous of degree $d^2 - d$. An element $u \in A'$ such that $\phi(u)$ is a diagonal matrix with distinct eigenvalues witnesses that this polynomial is not identically zero. □

Thus a semisimple matrix $u \in A$ such that the torus T generated by u is probably maximal (with error probability δ) can be found with $O(MM(n)\operatorname{polylog} n + SF_K(n) + R(A))$ operations. The error probability can be pushed under a prescribed bound ε by repeating this procedure $O(\log \frac{1}{\varepsilon})$ times independently, and taking the element which has minimal polynomial of maximal degree, see Lemma 1.

In the steps described in the rest of the section we assume that we are provided with an element u which generates a maximal torus T. We keep the notation introduced in Section 3 (C, S, H, N). We denote $\dim_K T$ by d.

6.3. Calculating C

We follow the method suggested by Theorem 11. First we calculate the subspace $L = [A, A] \cap T$. The next two lemmas provide us with a tool for generating random elements of L.

Lemma 15. *The map $a \mapsto J_s(\Phi_T a)$ is a linear map of A onto T and the map $a \mapsto J_n(\Phi_T a)$ is a linear map from A onto $Rad(H)$. Furthermore, $J_n(\Phi_T a) = a$, for every $a \in Rad(H)$, and $J_s(\Phi_T a) = a$, for every $a \in T$.*

Proof. We know that Φ_T is a linear projection of A onto H. Also, $\Phi_T Rad(A) = Rad(A)$ and J_s is zero on $Rad(H)$. By Wedderburn–Malcev, $H = T + N$, a direct sum of vector spaces. Let $\pi : H \to T$ and $\mu : H \to Rad(H)$ stand for projections corresponding to this decomposition. It remains to show that J_s and J_n (restricted to H) coincide with π and μ, respectively. For every $a \in H$, $\pi(a)$ is semisimple and $\mu(a)$ is nilpotent. Since H centralizes T, $\pi(a)$ commutes with a and the same holds for $\mu(a) = a - \pi(a)$. From the uniqueness of the Jordan decomposition we infer that $\pi(a) = J_s(a)$ and $\mu(a) = J_n(a)$. □

Lemma 16. $J_s(\Phi_T[A, A]) = L = [A, A] \cap T$.

Proof. Since $J_s(\Phi_T a)=a$ for every $a \in T$ it suffices to show that $J_s(\Phi_T a) \in [A,A]$ for every $a \in [A,A]$. By Corollary 2 $A=B+Rad(A)$ (direct sum as vector spaces) for some semisimple subalgebra $B \leq A$ containing T. Since $J_s(\Phi_T a)=0$ for every $a \in Rad(A)$ it is sufficient to prove the assertion for the semisimple algebra B in place of A. By Lemma 6 we have $T=C_B(T)$ hence $J_s(\Phi_T a)=\Phi_T a$ for every $a \in B$. We know that $\Phi_T a - a \in [T,B] \subseteq [B,B]$. Hence $\Phi_T a \in [B,B]$ if and only if $a \in [B,B]$. □

We calculate a basis L by generating sufficiently many random elements of the form $J_s(\Phi_T[a,b])$.

Lemma 17. *Let $k \leq \dim_K L$, $0<\varepsilon$, $\delta<1$, and let $h \geq k\lceil(\log k+\log \frac{1}{\varepsilon})/\log \frac{1}{\delta}\rceil$. Assume that the elements $a_{11},b_{11},\ldots,a_{1,h},b_{1,h},\ldots a_{d1},b_{d1},\ldots,a_{d,h}b_{d,h}$ are chosen independently from A according to a probability distribution satisfying condition $AlgRand(A,\dim_K L,\delta)$. Then with probability at least $1-\varepsilon$, the set $\{J_s(\Phi_T[a_{ij},b_{ij'}]) \mid i=1,\ldots,k,\ j,j'=1,\ldots,h\}$ contains at least k linearly independent elements of L.*

Proof. Let $l=\dim_K L$. By fixing a K-basis $b_1,\ldots,b_l$ of L we identify L with K^l. For a tuple $(y_1,z_1,\ldots,y_k,z_k) \in A^{2k}$ let Y stand for the $l \times k$ matrix the columns of which are $J_s(\Phi_T[y_{i,z_i}])$ $(i=1,\ldots,k)$. Let Γ be the family of all k-element subsets of $\{1,\ldots,l\}$. For each $\gamma \in \Gamma$ let $f_\gamma(y_1,z_1,\ldots,y_k,z_k)$ be the determinant of the $k \times k$ minor of Y which consists of the rows indexed by the elements of γ. Obviously f_γ is a multilinear function. We observe that all the functions f_γ $(\gamma \in \Gamma)$ vanish on a particular tuple $(y_1,z_1,\ldots,y_k,z_k) \in A^{2k}$ if and only if the elements $J_s(\Phi_T[y_i,z_i])$ $(i=1,\ldots,k)$ are linearly dependent over K. By Lemma 16 this cannot be the case for every $(y_1,z_1,\ldots,y_k,z_k) \in A^{2k}$ and hence there exists at least one $\gamma \in \Gamma$ such that f_γ is not identically zero. By Lemma 1 with probability at least $1-\varepsilon$ there exist indices $j_1,\ldots,j_k,j'_1,\ldots,j'_k$ such that $f_\gamma(a_1j_1,b_{1j'_1},\ldots,a_{kj_k},b_{kj'_k}) \neq 0$. Then the elements $J_s(\Phi_T[a_{1j_1},b_{1j'_1}]),\ldots,J_S(\Phi_T[a_{kj_k},b_{kj'_k}])$ are linearly independent. □

Like in Section 5, it will be convenient to perform calculations in T in terms of the basis $1,u,\ldots,u^{d-1}$. If it has not been done before we calculate the Frobenius normal form $Frob(u)$ of u together with a transition matrix b such that $b^{-1}ub=Frob(u)$ using Giesbrecht's method with $O(MM(n)\text{polylog}\, n)$ field operations. Then we can read the coordinates of an element $z \in T$ in terms of the basis $1,u,\ldots,u^{d-1}$ from the first column of the first block of $b^{-1}ub$.

We find a basis of L with $O(\log \frac{1}{\varepsilon}\dim_K L(MM(n)+R(A)+SF_K(n))\text{polylog}\, n)$ operations (even if $\dim_K L$ is not known a priori) as follows. Set $h=\lceil(\log d+\log \frac{d}{\varepsilon})/\log \frac{1}{\delta}\rceil$. For $k=1,2,4,\ldots,2^{\lceil \log_2 d\rceil}$ select a maximal linearly independent system from $\{J_s(\Phi_T[a_{ij},b_{ij'}]) \mid i=1,\ldots,k,\ j,j'=1,\ldots,h\}$ where a_i,b_i are random elements of A chosen independently according to a distribution which satisfies $AlgRand(A,d,\delta)$. We stop if we obtained less than k elements, otherwise we proceed with $2k$ in place of k. By the lemma, the probability that we stop with a system which does not generate L is at most ε.

Note that $A/Rad(A)$ is commutative iff $L=(0)$. Then $C=T$. Otherwise assume that we have a basis $b_1,\ldots,b_l$ of L. We choose linear function $f_1,\ldots,f_{d-l}: T \to K$ such that $L\cap_{i=1}^{d-l}\ker f_i$. Then $C=\{z \in T \mid zL \subseteq L\}=\{z \in T \mid f_i(zb_j)=0\ (i=1,\ldots,l,\ j=1,\ldots,d-l)\}$ whence we obtain a basis of C by solving a system of $l(d-l)$ linear equations in d variables. This costs $O(MM(d)l(d-l)/d) = O(dMM(d))$ operations. Finally we find an element $u' \in C$ which generates C as an algebra with identity by taking a random linear combination of these basis elements. (By Lemma 14, a random element of C will generate C. Note that we can verify whether u' generates C with $O(MM(d)\text{polylog}\, d)$ operations by testing linear independence of $1, u, \ldots, u^{\dim C-1}$.)

The total cost of the algorithm described in this subsection amounts to $O(\log \frac{1}{\varepsilon} d(MM(n)+R(a)+SF_K(n))\text{polylog}\, n)$ operations in K. If $A/Rad(A)$ happens to be commutative then $O(\log \frac{1}{\varepsilon}(MM(n)+R(a)+SF_K(n))\text{polylog}\, n)$ operations are sufficient.

6.4. Generating elements of N

Throughout this subsection we assume that we are provided with element u' which generates C as an algebra with identity.

Lemma 18. *Assume that $a_1,\ldots,a_m$ generate A as an algebra with identity. Then the elements $\{[u',a_1],\ldots,[u',a_m]\}$ generate ANA as an ideal of A.*

Proof. Let J be the ideal generated by $[u',a_1],\ldots,[u',a_m]$. Obviously $J \subseteq A[u',A]A \subseteq A[C,A]A = ANA$. Observe that $u'+J$ centralizes the generators a_i+J of the factor algebra A/J. Hence $[u',A] \subseteq J$ and since C is generated by u' we have $[C,A] \subseteq J$. By definition $N=[C,A]$. □

Hence generators of ANA can be calculated with $O(mMM(n))$ operations by taking $[u',g_1],\ldots,[u',g_m]$.

6.5. Generating elements of $Rad(H)$

We generate elements of $Rad(H)$ as follows. From a random element $a \in A$ we first calculate $\Phi_T a$ using the method described in Section 5. Then we compute the nilpotent part $J_n(\Phi_T a)$ of $\Phi_T a$. The cost is $O(MM(n)\text{polylog}\, n + SF_K(n))$ operations. Note that because of linearity of the map $a \mapsto J_n(\Phi_T a)$ (cf. Lemma 15) the method can be considered as a way to generate "random" elements of $Rad(H)$. To be more specific, if we choose a according to a distribution satisfying $AlgRand(A,D,\delta)$ then the distribution of $J_n(\Phi_T a)$ satisfies condition $AlgRand(Rad(H),D,\delta)$.

We are going to give an upper bound for the number of elements from $Rad(H)$ which – in addition to the generators of ANA – are sufficient to generate $Rad(A)$ as an ideal. The following elementary lemma is well known. A proof can be obtained by combining [17], Corollary 4.1b and Lemma 4.2.

Lemma 19. *Let B be finite dimensional K-algebra and $M \subseteq Rad(B)$. Then $Rad(B) = BMB$ if and only if $Rad(B) = BMB + Rad(B)^2$. In other words, the ideal generated by M is $Rad(B)$ if and only if the same holds modulo $Rad(B)^2$.*

Lemma 20. *Assume that $A/Rad(A)$ is a central simple K-algebra of dimension d^2. Then $Rad(A)$ as an ideal of A can be generated by $\lceil \dim_K Rad(A)/d^3 \rceil$ elements from $Rad(H)$. Furthermore, A as an algebra with identity cannot be generated by less than $\lceil \dim_K Rad(A)/d^4 \rceil$ elements.*

Proof. Let ψ stand for the natural projection $A \to A/Rad(A)^2$. Then $\psi(T)$ is a maximal torus in $A \to A/Rad(A)^2$. We have $C_{\psi(A)}\psi(T) = \Phi_{\psi(T)}(\psi(A)) = \psi(\Phi_T A) = \psi(H)$. In view of this together with Lemma 19 it is sufficient to prove the assertion for $A/(Rad(A))^2$ in place of A. In other words, we may assume that $Rad(A)^2 = (0)$. By Wedderburn–Malcev there exists a subalgebra $D \leq A$ such that $A = D + Rad(A)$ (direct sum as vector spaces). Assume that A is generated by $a_1, \ldots, a_m$. Let $a_i = b_i + c_i$ where $b_i \in D$ and $c_i \in Rad(A)$. One easily verifies that $c_1, \ldots, c_m$ generate $Rad(A)$ as an ideal. On the other hand, since $Rad(A)^2 = 0$ we have $Ac_iA = (D + Rad(A))c_i(D + Rad(A)) = Dc_iD$, whence $\dim_K Ac_iA \leq (\dim_K D)^2 = d^4$. This implies the inequality $m \geq \lceil \dim_K Rad(A)/d^4 \rceil$.

To prove the first assertion we use a refinement of the argument of the proof of Theorem 10. We consider $Rad(A)$ as a $D \otimes_K D$-module in the natural way. Then ideals of A contained in $Rad(A)$ are exactly the $D \otimes_K D$-submodules and elements b of $Rad(H) = Rad(A) \cap C_A(T)$ are characterized as $(1 \otimes a)b = (a \otimes 1)b$ for every $a \in T$. We know that $D \otimes_K D \cong M_{d^2}(K)$ and $Rad(A)$ as a $D \otimes_K D$-module is isomorphic to D^h, the direct sum of h copies of the simple $D \otimes_K D$-module D (with the natural module structure). Here $h = \dim_K Rad(A)/d^2$. We claim that if $a_1, \ldots, a_r$ are linearly independent elements of D then $(a_1, \ldots, a_r)$ generates the $D \otimes_K D$-module D^r. This can be verified at once if we identify $D \otimes_K D$ with $M_{d^2}(K)$ and D with the standard $M_{d^2}(K)$-module K^{n^2}. Let $r \leq d$ and choose r linearly independent elements $a_1, \ldots, a_r$ from T. Then by the claim $b = (a_1, \ldots, a_r)$ generates D^r as a $D \otimes_K D$-module and $(1 \otimes a)b = (a_1a, \ldots, a_ra) = (aa_1, \ldots, aa_r) = (a \otimes 1)b$. Hence $\lceil h/d \rceil$ generators of $Rad(A)$ with the required property can be constructed by distributing the irreducible summands of $Rad(A)$ into appropriate blocks and taking a single generator in each block. □

Corollary 21. *Assume that A as an algebra with identity is generated by m elements. Suppose that the simple components of $A/Rad(A)$ are $\widetilde{A}_1, \ldots, \widetilde{A}_r$ with $\dim_K \widetilde{A}_i / \dim_K Z(\widetilde{A}_i) = d_i^2$. Then there exists a subset $M \subseteq Rad(H)$ of size at most*

$$\max\{\min(md_i, \lceil \dim_K A/d_i^3 \rceil) \mid i = 1, \ldots, r\} \leq \lceil (\dim_K A)^{\frac{1}{4}} m^{\frac{3}{4}} \rceil \leq \lceil n^{\frac{1}{2}} m^{\frac{3}{4}} \rceil$$

such that $A(M + N)A = Rad(A)$.

Proof. As in the proof of Lemma 20 we can assume that $Rad(A)^2 = (0)$. Then $N^2 = (0)$ as well and by Proposition 7, N is an ideal of A. Hence $S \cong A/N$ and S is also generated by m elements. This means that for the rest of the proof we may further assume that

$N = (0)$, or, equivalently, $A = S$. By Proposition 9, A is a direct sum of subalgebras $A_1, \ldots, A_r$, where $A_i/Rad(A_i) \cong \widetilde{A}_i$. Assume that $M_i \subseteq Rad(H_i) = Rad(H) \cap H_i$ such that $A_i M_i A_i = Rad(A_i)$ $(i = 1, \ldots, r)$. It is easy to construct a set $M \subseteq Rad(H)$ of cardinality $\max |M_i|$ such that for every $i \in \{1, \ldots, r\}$ $\pi_i(M) = M_i$ where $\pi_1, \ldots, \pi_r$ are the projections corresponding to the direct decomposition of A. It is immediate that such an M generates $Rad(A)$ as an ideal. Hence it is sufficient to prove the assertion in the special case where $\widetilde{A} = A/Rad(A)$ is a simple K-algebra. Then C is a field in $Z(A)$ and we can consider A as a C-algebra. The statement now follows from Lemma 20, applied to A as a C-algebra. (The bound independent of the d_is is obtained by taking an appropriate weighted geometric mean of md_i and $\dim_K A/d_i^3$.) □

The next lemma gives a bound on the random elements of $Rad(H)$ which probably generate $Rad(A)$ modulo the ideal AMA. We omit the proof which is rather technical and can be carried out in a fashion similar to the proof of Lemma 17.

Lemma 22. *Assume that there exists a subset $M \subseteq Rad(H)$ of size k such that $A(M+N)A = Rad(A)$. Let $0 < \varepsilon$, $\delta < 1$ and $h \geq k\lceil(\log k + \log \frac{1}{\varepsilon})/\log \frac{1}{\delta}\rceil$. Assume that the elements $a_1, \ldots, a_h \in A$ are chosen independently according to a probability distribution satisfying $AlgRand(A, \dim_K Rad(A), \delta)$. Then with probability at least $1 - \varepsilon$ the subspace $N \cup \{J_n(\Phi_T a_i) \mid i = 1, \ldots, h\}$ generate $Rad(A)$ as an ideal of A.*

6.6. Computing $Rad(A)$

Here we summarize the algorithm for computing $Rad(A)$. The input consists of matrices $g_1, \ldots, g_m$ such that A is the matrix algebra generated by the identity matrix and $g_1, \ldots, g_m$. We assume that random elements of a are generated independently according to a probability distribution satisfying condition $AlgRand(A, n^2, \delta)$ for a constant $0 < \delta < 1$, say $1/2$. An error probability bound $0 < \varepsilon < 1$ is also given as a part of the input. We require that each of the three big steps which make use of randomization of the algorithm works correctly with probability at least $1 - \frac{\varepsilon}{3}$.

First we find a semisimple matrix u which generates a maximal torus T by the method of Section 6.2. Then we calculate the subalgebra $C \leq T$ (and a generator u' of C) using the method described in Section 6.3. If $C = T$ then we set $k = m$ otherwise $k = \lceil n^{\frac{1}{2}} m^{\frac{3}{4}} \rceil$. Then we calculate the commutators $[u', g_i]$ $(i = 1, \ldots, m)$ as well as $J_n(\Phi_T a)$ for $O(\log \frac{1}{3\varepsilon} k \log k)$ random elements $a \in A$. (The exact constant is given in Lemma 22.) These elements generate $Rad(A)$ with probability at least $1 - \varepsilon$. We obtained the following.

Theorem 23. *Let $A \leq M_n(K)$ be given by m generators and $0 < \varepsilon < 1$. Then a system of matrices which generate $Rad(A)$ with probability at least $1 - \varepsilon$ as an ideal of A can be computed by a probabilistic algorithm which performs $O((n + n^{\frac{1}{2}} m)(MM(n) + SF_K(n) + R(A))\text{polylog}\, n \log \frac{1}{\varepsilon})$ operations in K. If $A/Rad(A)$ is commutative then the algorithm performs $O(m(MM(n) + SF_K(n) + R(A))\text{polylog}\, n \log \frac{1}{\varepsilon})$ operations.*

We conclude with some remarks. We assume that $\mathrm{char}\, K = 0$, ε is a constant and m is small, say $m = \mathrm{O}(\log n)$. Then the cost of the algorithm is $\mathrm{O}(nMM(n)\mathrm{polylog}\, n) = \mathrm{O}(n^4)$ operations provided that we can efficiently select random elements (i.e., $R(A) = \mathrm{O}(MM(n)\mathrm{polylog}\, n)$. This is definitely better than the cost of the so far only known method by Friedl and Rónyai [12] which appears to be around $\mathrm{O}(n^6)$ or even more.

Note that for applications it seems to be important to exhibit a single nonzero element of $Rad(A)$ (provided that $Rad(A) \neq (0)$). For this task an algorithm of complexity around $\mathrm{O}(MM(n))$ could be considered optimal. By a version of the algorithm presented here we can almost achieve this bound in the special cases where $Rad(H) \neq (0)$ or $A/Rad(A)$ is (nearly) commutative. In the general case computation of the subalgebra C with its complexity roughly $\mathrm{O}(nMM(n))$ appears to be the weakest point of the present algorithm. It would be desirable to have a more efficient method for computing C or for treating algebras with $Rad(H) = (0)$ in another way.

Acknowledgements

The author is indebted to Kati Friedl, Lajos Rónyai and the anonymous referee for their useful remarks and suggestions.

References

[1] L. Babai, R. Beals, J.-Y. Cai, G. Ivanyos, E.M. Luks, Multiplicative equations over commuting matrices, Proc. 7th ACM-SIAM Symp. on Discrete Algorithms, 1996, pp. 498–507.
[2] L. Babai, K. Friedl, M. Stricker, Decomposition of $*$-closed algebras in polynomial time, Proc. ISSAC'93, 1993, pp. 86–94.
[3] J.R. Bastida, Field extensions and Galois theory, in: G.-C. Rota (Ed.), Encyclopedia of Mathematics and Its Applications, vol. 22, Cambridge University Press, Cambridge and Addison-Wesley, Reading, MA, 1984.
[4] D. Bini, V. Pan, Polynomial and matrix computations, vol. 1 (Fundamental Algorithms), Birkhäuser, Basel, 1994.
[5] A.M. Cohen, G. Ivanyos, D.B. Wales, Finding the radical of an algebra of linear transformations, Proc. MEGA'96, J. Pure Appl. Algebra 117–118 (1997) 177–193.
[6] C.W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Wiley, New York, 1962.
[7] W.A. de Graaf, Using Cartan subalgebras to calculate nilradicals and Levi subalgebras of Lie algebras, J. Pure Appl. Algebra 139 (1999) 25–39.
[8] W.A. de Graaf, G. Ivanyos, Finding maximal tori and splitting elements in matrix algebras, Manuscript, 1998.
[9] W.M. Eberly, Computations for algebras and group representations, Ph.D. thesis, Dept. Comput. Sci., Univ. Toronto, 1989.
[10] W.M. Eberly, M. Giesbrecht, Efficient decomposition of associative algebras, Proc. ISSAC'96, 1996, pp. 170–178.
[11] K. Friedl, Decomposition of matrix groups and algebras, Ph.D. thesis, University of Chicago, 1994.
[12] K. Friedl, L. Rónyai, Polynomial time solution of some problems in computational algebra, Proc. 17th ACM STOC, 1985, pp. 153–162.
[13] M. Giesbrecht, Nearly optimal algorithms for canonical matrix forms, SIAM J. Comput. 24 (1995) 948–969.
[14] D.F. Holt, S. Rees, Testing modules for irreducibility, J. Austral. Math. Soc. Ser. A 57 (1994) 1–16.

[15] A. Kertész, Lectures on Artinian rings, Akadémiai Kiadó, Budapest 1987.
[16] D.E. Knuth, The Art of Computer Programming, vol. 2, Seminumerical Algorithms, 2nd ed., Addison-Wesley, Reading, MA, 1981.
[17] R.S. Pierce, Associative Algebras, Springer, Berlin, 1982.
[18] L. Rónyai, Computing the structure of finite algebras, J. Symbolic Comput. 9 (1990) 355–373.
[19] J.T. Schwartz, Fast probabilistic algorithms for verification of polynomial identities, J. ACM 27 (1980) 701–717.
[20] A. Seidenberg, Constructions in algebra, Trans. Amer. Math. Soc. 197 (1974) 273–313.
[21] D.J. Winter, Abstract Lie Algebras, MIT Press, Cambridge, MA, 1972.
[22] R.E. Zippel, Probabilistic algorithms for sparse polynomials, Proc. EUROSAM '79, Lecture Notes in Computer Science, vol. 72, Springer, Berlin, 1979, pp. 216–226.